INTERNAL AUDIT
CONTROLS EVALUATION
INFORMATION CENTER

December 3, 2001

Roanoke City Council Audit Committee
Roanoke, Virginia

We have completed an audit of the Department of Technology's user support function. The audit was performed in accordance with generally accepted government auditing standards.

BACKGROUND

Workstation support was incorporated into the Information Center, which was created in March 2001 as part of the reorganization of the Department of Technology. The Information Center has eight permanent full time and four temporary full time positions responsible for providing user support and training. This staff is responsible for setting-up and installing personal computers under the City's PC replacement program. They also review and approve requests to purchase other technology equipment and software in order to ensure City standards are maintained and the technology is compatible with the City's current systems. The Information Center operates a "help desk" during normal office hours to troubleshoot user problems and take user requests for services. On average, the Center receives 471 calls a month, or 109 calls a week. It provides support for approximately 1,000 desktop and laptop computers, as well as a number of printers, hand-held computers, and other peripheral equipment. The Information Center is also responsible for setting up and deleting user access to the City's network and mainframe systems, but is not responsible for administering access security for applications on the network and mainframe. The Information Center also has a trainer on staff to train users and provide support for personal computer applications (Lotus, Microsoft, and Corel Word Perfect).

In November 2000, the C: Support Call Management system was installed to improve operational management of the support and help desk functions. This system is a network based, shared database system that allows the help desk to quickly enter a problem, search for solutions, and to establish and route service requests as necessary. The system notifies technicians and the Information Center Coordinator when a service request remains open past a standard time for resolving the request. The system serves as a repository of data regarding technology and user problems and work performed to address problems. The C: Support system includes an asset management database on which the Information Center maintains an inventory of CPUs and laptops in the City organization. The system is fully searchable and allows management to easily monitor support staff performance, problematic hardware and software, and user training needs.

PURPOSE

The purpose of this audit was to evaluate the design and operation of the system of internal controls that ensures users receive effective and timely support and to evaluate the controls related to security issues addressed by the Information Center.

METHODOLOGY

We gained an understanding of the help desk area through a review of existing documentation and interviews with the Information Center. Based on the information, audit tests were developed to evaluate the operation of controls.

SCOPE

We reviewed controls in place as of August 31, 2001, and analyzed C: Support's data transactions from January 1, 2001, to September 30, 2001.

RESULTS

During the audit, we found the staff and management in the Information Center utilized the C: Support system effectively in carrying out their support responsibilities. The staff consistently maintains complete data on the system and management uses the data to plan training curriculum and monitor service. The staff and management appear to work well together as a team. Our review of service requests found that calls were addressed in accordance with department protocol and that appropriate and timely service was provided in most all cases. We did note findings in the area of access control and asset security.

Finding 01

People can enter an unlimited number of incorrect passwords when attempting to log onto the City's network. This increases the risk that an unauthorized person may be able to guess a password and gain entry onto the network. Also, users who forget their network or mainframe password can call the Information Center and ask that their password be reset. There are no procedures in place to confirm the caller's identity, increasing the risk that a person could gain unauthorized access to City systems.

Recommendation 01

The Information Center should enable the function on all user accounts on the network that locks out the user after entering three consecutive incorrect passwords. The Information Center should also establish a requirement that the function be enabled whenever new accounts are set-up. The Information Center should establish a new procedure for authenticating callers before resetting a password.

Management Response 01

When new Novell (ie., network) accounts are established, the three-missed password restriction will be enabled. This procedure will be documented in the Information Center Policies and Procedures and communicated to Information Center staff immediately. The procedure will also be shared with Department of Technology Technical Support staff, as they serve as the Information Center's backup for setting up new Novell accounts.

All existing Novell accounts will be edited to include the three-missed password restriction. These modifications will begin immediately and will be completed by January 2, 2002.

When customers call the helpdesk to have passwords reset, Information Center staff will verify the caller name, department name, and telephone number. Information Center staff will then inform the caller that, for security reasons, we must call them back and we will reset the password with a successful callback. This procedure will be documented in the Information Center Policies and Procedures and communicated to Information Center staff immediately. This procedure will also be shared with Department of Technology Technical Support and Operations staff, as both of these areas have the ability to reset end user passwords in some application areas.

Finding 02

User identifications for terminated employees were active on the network, mainframe, and lotus notes. A terminated employee or someone knowing that employee's user identification could manipulate records, execute transactions, or view confidential information without authorization and without being detected depending on access level and circumstances.

Department managers are responsible for notifying the Department of Technology when an employee's system access should be removed for any reason. The administrative procedures do not highlight the steps to be taken when an employee terminates and does not specify how the Department of Technology is to be notified.

Recommendation 02

The Department of Technology should revise the System Request Access form, so that it can also be utilized to delete user identifications for terminated employees as well as set-up access for new employees. Human Resources should revise the administrative procedure for terminating employees to more clearly state the steps to be taken by departments when an employee terminates. The steps should include submitting the system access form to the Information Center. The Information Center should be included as one of the departments to be notified during the termination process once this process is adopted as a Lotus Notes workflow.

Management Response 02

The Information Center will modify the paper version of the System Access Request form so that it can be used both for instatement and termination of access by December 3, 2001. Instructions for use of this form will be communicated to all departments via memorandum by December 7, 2001.

Department of Technology's e-business group will continue work on the Lotus Notes workflow version of the System Access form. Upon it's completion, this process will replace the paper version of the System Access form for those using Lotus Notes. Departments without access to Lotus Notes will continue to use the paper version of the System Access form.

The Information Center will remove access for those employees on the terminated employees lists in the Lotus Notes employee telephone directory. This listing will be checked within two business days of the payroll run date and access will be terminated, with written notification given to the terminated employee's department manager, within five business days of the employee's termination date. The information center will establish a lists of systems to which an employee could have access and will review this list when processing access termination for an employee.

Human Resources Response: Human Resources will revise Administrative Procedure 2.7 "Terminating an Employee" to include more specific instructions to be followed when terminating employees. The revision will specify that department managers must complete a System Access Request form for the Information Center in the Department of Technology when terminating an employee with Lotus Notes, Novell, or mainframe access.

Finding 03

We noted that departments are allowed to purchase their own technology equipment after the Information Center reviews the proposed purchase and approves it. Departments are not required to notify the Information Center after they receive the equipment which results in some computers not being added to the C: Support Asset Management system. Laptops are primarily the assets that do not get reported because departments are able to use those without additional set-up and without getting a network connection that would require Information Center involvement. We selected ten approved requests from the Information Center's files and found that the computers were purchased. Of the ten computers purchased, five (1 desktop and 4 laptops) were not listed in C: Support's Asset Management system.

The Information Center is in the process of taking a complete physical inventory and adding computers not currently listed on the C: Support Asset Management system.

Recommendation 03

We recommend that the Information Center print a report of desktop and laptop computers by department and location once each year using the C: Support Asset Management system. The Information Center should send the reports to the user departments with an explanatory memo requiring departments to review the report and verify the accuracy of the report. The departments should add the necessary information for any computer not listed and return the report to the Information Center for entry into the C: Support Asset Management system.

Management Response 03

The Information Center will continue to verify and update asset records on each desktop CPU and laptop as new installations and/or moves require. The Information Center will produce an annual inventory report for each department requesting a review and update, if necessary. This report should be returned to the Information Center so that the asset records can be updated. The first annual inventory reports will be sent to departments in September 2002.

CONCLUSION

The Information Center's system of internal controls is adequate to ensure users receive effective and timely support. The system of internal controls does not adequately address security risks related to access control.

We would like to thank the Information Center for its cooperation and assistance during the audit.

_____
Pamela Mosdell
Senior Auditor

_____
Drew Harmon, CPA, CIA
Municipal Auditor